(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年7 月14 日 (14.07.2005)

PCT

(10) 国際公開番号
WO 2005/064485 A1

(51) 国際特許分類[7]: G06F 15/00, 1/00

(21) 国際出願番号: PCT/JP2003/016815

(22) 国際出願日: 2003 年12 月25 日 (25.12.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 三井物産株式会社 (MITSUI & CO., LTD.) [JP/JP]; 〒100-0004 東京都 千代田区 大手町一丁目２番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 大島 俊一 (OSHIMA,Shunichi) [JP/JP]; 〒270-0176 千葉県 流山市 加３−６−１ 四番館９０５ Chiba (JP). 斉藤 晃 (SAITO,Hikaru) [JP/JP]; 〒112-0015 東京都 文京区 目白台１−９−４−３０８ Tokyo (JP). 中里 昇吾 (NAKAZATO,Shogo) [JP/JP]; 〒110-0004 東京都 台東区 下谷２−１９−５−２０２ Tokyo (JP). 奈良原 智明 (NARAHARA,Tomoaki) [JP/JP]; 〒167-0054 東京都 杉並区 松庵１−３−１６ Tokyo (JP). 吉川 治宏 (KIKKAWA,Haruhiro) [JP/JP]; 〒154-0022 東京都 世田谷区 梅丘１−５５−２ Tokyo (JP). 勝原 透匡 (KATSUHARA,Yukimasa) [JP/JP]; 〒135-0091 東京都 港区 台場１−３−４−１５０２ Tokyo (JP). 荻 猛 (OGI,Takeshi) [JP/JP]; 〒156-0054 東京都 世田谷区 桜丘５丁目７番１１号 Tokyo (JP).

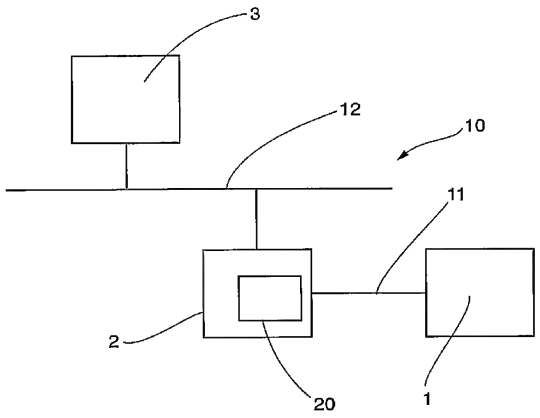
(74) 代理人: 市原 俊一, 外 (ICHIHARA,Shunichi et al.); 〒160-0004 東京都 新宿区 四谷２丁目８番地 コーポクローバ浜５０５号 Tokyo (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK,

[続葉有]

(54) Title: PORTABLE PERSONAL SERVER WITH BIOLOGICAL INFORMATION RECOGNIZER

(54) 発明の名称: 生体情報認識装置を備えた携帯型パーソナルサーバ装置



(57) Abstract: A portable personal server (1) connectable through a network (11) with a PC (2) connected with an external network (12) and permits communication with the PC (2) only when user's fingerprint information read out by means of a fingerprint authentication unit (22) matches registered information. In order to communicate through the network (11), the portable personal server (1) and the PC (2) acquires an address using APIPA so that the collision of address does not take place in the external network (12). Consequently, the portable personal server (1) also functions as a network server on the external network (12). A portable personal server exhibiting high confidentiality of data and suitable for central management of data can thereby realized.

(57) 要約: 携帯型パーソナルサーバ装置（１）は、外部ネットワーク（１２）に接続されたＰＣ（２）にネットワーク（１１）を介して接続可能であり、指紋認証装置（２２）により使用者の指紋情報を読み取り、登録情報と一致した場合のみＰＣ（２）との通信を許可する。携帯型パーソナルサーバ装置（１）とＰＣ（２）とは、ネットワーク（１１）を介して通信するために、外部ネットワーク（１２）とアドレスの衝突が起こらないようAPIPAを用いてアドレスを取得する。この結果、携帯型パーソナルサーバ装置（１）は外部ネットワーク（１２）上のネットワークサーバとしても機能する。データの機密性が高く、データを一元管理するのに適した携帯型パーソナルサーバ装置を実現できる。

WO 2005/064485 A1

LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (広域): ARIPO 特許 (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明細書

生体情報認識装置を備えた携帯型パーソナルサーバ装置

技術分野

本発明は、ネットワーク接続手段を備えた通信端末と通信することにより、当該通信端末のネットワーク接続手段によって接続されたネットワークとの間でデータ交換などの処理を行うことのできるサーバ機能を有する生体情報認識装置を備えた携帯型パーソナルサーバ装置に関するものである。

背景技術

ビジネスおよび日常で必要となる情報は、電子データとしてパーソナルコンピュータ（ＰＣ）の内部記憶装置、ネットワークに接続されたサーバシステム、あるいはＰＣに対する外部接続記憶装置などに格納されている。そして、これらのデータへのアクセスおよびデータの処理にはＰＣが広く一般的に使用されている。

近年、インターネットの普及により、あらゆる場所に設置されたＰＣからネットワークを介して必要なデータにアクセスすることが可能になった。そのため、ユーザは、データが必要になった時に、傍にあるＰＣを利用してネットワークに接続して、必要なデータにアクセスするようになっている。この結果、１人のユーザが、オフィスに設置されているＰＣ、出張など外出時に使用する携帯型ＰＣ、自宅に設置されているＰＣなど、２、３台のＰＣを使用することが一般的に行なわれている。一方で、オフィスや家庭に設置されたＰＣを複数のユーザが共同で利用することも行なわれている。

また、情報への常時アクセスの必要性が高まるにつれ、ＰＤＡや携帯電話といった情報処理端末へデータをコピーして常時携帯するといったことも行われている。単にデータを常時携帯するための手段としては、ＵＳＢトークン、メディアカードなどのストレージデバイスが用いられている。

ここで、ＰＣや情報処理端末へデータを無制限にコピーすることは情報の漏洩に直結する。したがって、データに対するアクセス権を識別するための手段として、パスワードや生体情報を用いた端末アクセス制御技術が用いられている。

このような端末アクセス制御技術を有するＰＣとしては、指紋認証カードをＰＣスロットに差込んだ後、自分自身のＰＣとして使用するミニコンピュータが案出されている（例えば、特許文献１参照。）。また、指紋センサを搭載することにより、本人認証およびセキュリティ機能を提供するＰＤＡが案出されている（例えば、特許文献２参照。）。

［特許文献１］特開平１１－２７２３４９号公報

［特許文献２］米国特許第６０１６４７６号明細書

発明の開示

（発明が解決しようとする課題）

１人のユーザが複数のＰＣを利用してネットワークを介してデータへのアクセスを行うようになった結果、アクセスしたデータが複数のＰＣに分散して格納されてしまうことが頻繁に発生している。また、ユーザがアクセスしたデータに処理を施した場合には、処理前のデータと処理後のデータが異なるＰＣに分散して保持されてしまい、一つの情報の一貫性が保持できない。

そこで、ネットワークに接続されているサーバにデータを一元的に集めて保存、あるいは処理を行えば、比較的容易に情報の一貫性を保つことができる。この場合には、サーバをユーザ自身が管理することは容易ではないため、他人が管理するサーバに、当該サーバの能力および管理者を信頼して対価を支払ってデータを預けることになる。

しかし、個々のユーザ自身だけがアクセスすればよい個人データを、物理的に離れており、かつ、自らの管理下にないサーバに預けることは不安であり、コストもかかる。また、ネットワークに接続されているサーバは通常多数のユーザによって共有されている。したがって、どのような安全手段を施したとしても、必然的に当

該サーバにアクセス可能な他人に情報が漏洩する危険性が高い。また、ネットワークへのアクセスが不可能な場合には、当該サーバへのアクセスができず、必要なデータを必要な時に取得することが不可能になってしまう。

また、ＰＣを複数のユーザで共有する場合には、ユーザ同士が物理的に同じ記憶装置にデータを保存するために、ＰＣを共有する他のユーザに対してデータが漏洩する危険性が高い。

情報処理端末でデータを携帯する場合には、情報処理端末の操作性が、一般的にＰＣより劣り、汎用性も低いので、通常はＰＣを主端末として用いて情報処理端末は補助端末として用いている。この結果、ユーザは主端末であるＰＣと補助端末である情報処理端末との間のデータフォーマットの変換、データの一貫性の維持などに悩まされる。

携帯型の記憶媒体、例えばストレージデバイスでデータを携帯する場合には、ネットワークに接続されたサーバや、その他のネットワーク機器は、当該ストレージデバイスと直接通信を行うことが出来ない。したがって、ユーザは一旦ＰＣにストレージデバイスに格納されたデータを移動し、その後、ＰＣからネットワークにデータを送信するといった煩雑な操作をすることとなる。この結果、ＰＣにデータのコピーが残ってしまう場合があり、情報が漏洩する危険性がある。

一方、認証用デバイスによりＰＣを自分自身のＰＣとして使用する場合には、認証用のデバイスは、単に認証情報をＰＣに流し、ＰＣ上の指定されたサービスを起動するために用いられている。また、これら認証用デバイスから提供されるサービスは通常固定されており、専用ＣＰＵを搭載するものではアップデートが可能とされている。しかし、その場合でも数百キロバイト程度の非常に限定的なサービス書き込みエリアしか提供されていない。また、メーカー独自のＡＰＩを使ってプログラミングをする必要がある等、これら認証用デバイスが提供するサービスは実質的にはメーカー側が提供するサービスに限定されているのが現状であり、拡張性が乏しい。

次に、企業の秘密データなどを企業が従業員と交換する場合には、企業のシステ

ム担当者は自社ネットワーク内におけるデータの移動、処理に関しては、当該担当者の管理ポリシに従って管理することが出来る。しかし、一旦自社ネットワークの外部に移動したデータについては管理ポリシを徹底させることは困難である。例えば、従業員が自宅に設置されたＰＣを用いてアクセスし、取得した情報について社内の管理ポリシを適用することは難しく、従業員の良識に依存するしかない。

本発明の課題は、このような点に鑑みて、データを一元的に管理するために、ネットワーク接続手段を備えた通信端末と通信することにより、当該通信端末のネットワーク接続手段によって接続されたネットワークとの間でデータの処理が可能なサーバ機能を有する携帯型パーソナルサーバ装置を提案することにある。

（課題を解決するための手段）

上記の課題を解決するために、本発明の携帯型パーソナルサーバ装置は、

ネットワーク接続手段を備えた通信端末との間でデータ処理を行うローカルサーバ手段と、

前記通信端末のネットワーク接続機能によって当該通信端末に接続されたネットワークとの間で、データ処理を行うネットワークサーバ手段と、

生体情報に基づき個人認証を行う個人認証手段と、

前記個人認証手段により認証された場合にのみ、前記ローカルサーバ手段および前記ネットワークサーバ手段を利用可能にする制御手段とを有していることを特徴としている。

本発明の携帯型パーソナルサーバ装置は、ネットワーク接続手段を備えた通信端末との間でデータ処理を行うローカルサーバ手段を有している。すなわち、ＰＣなどのネットワーク接続手段を備えた通信端末と通信することによりローカルサーバとして機能するので、あらゆる場所に設置されているＰＣを用いて携帯型パーソナルサーバ装置に格納されたデータにアクセスすることができる。さらに、ＰＣによりデータ処理を施した場合でも、処理後のデータを常に携帯型パーソナルサーバ装置に保存して最新のデータに更新することができる。その結果、複数のＰＣにデー

タが散在することはなくデータの一貫性が保たれる。データのフォーマットを気にする必要もない。また、複数のＰＣにデータが散在することがないので携帯型パーソナルサーバ装置の管理を徹底することにより、企業等の管理ポリシに従ってデータを管理することができる。

また、本発明の携帯型パーソナルサーバ装置は、通信端末に接続されたネットワークとの間でデータの処理を行うネットワークサーバ手段を有している。従って、携帯型パーソナルサーバ装置からネットワークに向けて情報を発信することができ、ネットワークからのデータを受け取り、自動処理を行い、指定された通信端末装置に向けて処理結果を返すといった動作も可能である。また、携帯型パーソナルサーバ装置は、通信端末を介してネットワークに接続されているが、携帯型パーソナルサーバ装置自体がネットワークサーバ機能を有しているので、当該通信端末に一時的であってもデータが保存されることがない。このため、当該通信端末に保存されたデータから情報が漏洩してしまうことがない。

さらに、本発明の携帯型パーソナルサーバ装置は、指紋などの生体情報に基づき個人認証を行う個人認証手段と、この個人認証手段により認証された場合にのみ、前記ローカルサーバ手段および前記ネットワーク手段を利用可能にする制御手段とを有している。したがって、持ち主以外は携帯型パーソナルサーバ装置に蓄積されたデータにアクセスすることができない。このため、携帯型パーソナルサーバ装置を紛失した場合でも、他者へのデータの漏洩を避けることができる。特に、携帯型パーソナルサーバ装置は一切の操作用の入出力装置（キーボード、ディスプレイなどの装置）を持たない構成とすることができる。このようにすれば、携帯型パーソナルサーバ装置を紛失した場合において、他人が内部データにアクセスすることが困難であり、機密性が高い。

また、個人認証手段により携帯型パーソナルサーバ装置の持ち主を特定した上で、固有の電子証明書などを利用したネットワーク認証手段によって携帯型パーソナルサーバ装置をネットワークサーバとして機能させる。この結果、ネットワークからネットワークサーバとして機能している携帯型パーソナルサーバ装置へアクセスし

ようとする他人は、当該携帯型パーソナルサーバ装置が間違いなく当該携帯型サーバの持ち主のものであることを確認できる。また、当該携帯型サーバの持ち主本人が携帯型パーソナルサーバ装置を使用中であることも確認できるので、悪意のある者によって運用されたネットワークサーバへアクセスする危険性を減らすことができる。さらに、仮に携帯型パーソナルサーバ装置へアクセス中に問題が発生した場合、問題の発生原因が当該携帯型パーソナルサーバ装置および持ち主に起因するものであると特定することができるので、通信システムの信頼性を確保できる。

ここで、個人認証手段は、指紋センサなどの生体情報認識装置を備え、当該生体情報認識装置により読み込まれた読込生体情報が予め登録されている登録生体情報に一致するか否かにより個人認証を行うように構成することができる。

また、本発明の携帯型パーソナルサーバ装置は、格納データを前記読込生体情報を用いて暗号化するデータ暗号化手段を有していることが望ましい。持ち主の生体情報に基づいて携帯型パーソナルサーバ装置に格納されるデータが暗号化されているので、携帯型パーソナルサーバ装置を分解して内部のデータにアクセスしようとした場合でも、格納されているデータを他人が解読することは困難あり、他人へのデータの漏洩を避けることができる。

さらに、本発明の携帯型パーソナルサーバ装置は、前記読込生体情報が前記登録生体情報に一致した場合に、前記読込生体情報に基づいて公開鍵暗号方式に用いられる鍵の生成と保管を行い、当該鍵を用いて送信されるデータを暗号化する通信暗号化手段を有していることが望ましい。通信暗号化手段により、ネットワークを介してデータの送受を行なう場合のデータが保護されるので、通信システムのセキュリティが確保される。

さらにまた、本発明の携帯型パーソナルサーバ装置は、前記通信端末に接続するための通信ケーブル端子を有しており、この通信ケーブル端子を介して前記通信端末から電源の供給を受けるようになっていることが望ましい。電源がＰＣなどの通信端末の側から供給されるので、携帯型パーソナルサーバ装置は自己電源を持つ必要がない。この結果、携帯型パーソナルサーバ装置を小型で安価に製造することが

できるので、個々のユーザが常時携帯するのに便利である。また充電等の必要もない。さらに、物理的な手段で携帯型パーソナルサーバ装置と通信端末を通信可能に接続するので携帯型パーソナルサーバ装置と通信端末との間の通信を盗聴される危険性が少ない。

この場合、前記通信ケーブル端子をＵＳＢ接続端子とすることが望ましい。

図面の簡単な説明

図１は、本発明の携帯型パーソナルサーバ装置を用いて構築した通信システムの一例を示す全体構成図である。

図２は、図１の携帯型パーソナルサーバ装置のシステム構成図である。

図３は、図１の携帯型パーソナルサーバ装置の外観斜視図である。

図４は、図１の携帯型パーソナルサーバ装置のソフトウェア構成を表す概念図である。

(符号の説明)

１　携帯型パーソナルサーバ装置

２　ＰＣ

３　外部サーバ

１０　通信システム

１１　ネットワーク

１２　外部ネットワーク

２０　リレーサービス

２１　ＣＰＵ

２２　指紋認証装置

２３　通信インタフェース

２３ａ　接続端子

２４　メモリ

２５　ストレージメディアカードスロット

２６　フラッシュＲＯＭ

２７　指紋センサ部分

２８　ＵＳＢケーブル

３１　装置本体

４１　オペレーティングシステム

４２　指紋認証プログラム

４３　サーバプログラム

４４　暗号プログラム

発明を実施するための最良の形態

（全体構成）

図１は、本発明を適用した通信システムの一例を示す全体構成図である。図１に示すように、本形態の通信システム１０は、携帯型パーソナルサーバ装置１と、ネットワーク接続手段を備えたＰＣ２とを有しており、携帯型パーソナルサーバ装置１とＰＣ２とはネットワーク１１により通信可能に接続されている。ＰＣ２はインターネットなどの外部ネットワーク１２に接続されている。ネットワーク１１および外部ネットワーク１２はいずれもＩＥＥＥ８０２ネットワークであり、ＴＣＰ／ＩＰで接続されている。外部ネットワーク１２には外部サーバ３が接続されている。

（携帯型パーソナルサーバ装置の構成）

図２は携帯型パーソナルサーバ装置のシステム構成図である。携帯型パーソナルサーバ装置１は、ＣＰＵ２１、指紋認証装置２２、通信インタフェース２３、メモリ（ＲＡＭ）２４、ストレージメディアカードスロット２５、フラッシュＲＯＭ２６を有している。フラッシュＲＯＭ２６には、オペレーティングシステム（ＯＳ）４１、指紋認証プログラム４２、サーバプログラム４３、暗号プログラム４４が記憶されている。

図３は携帯型パーソナルサーバ装置の外観斜視図である。携帯型パーソナルサー

バ装置１は、手のひら大の大きさの卵形の輪郭形状をした装置本体３１を備え、装置本体３１の表面中央部分には指紋認証装置２２の指紋センサ部分２７が配置されている。装置本体３１の先端部には通信インタフェース２３の接続端子２３ａが配置されている。通信インタフェース２３はＵＳＢ通信インタフェースであり、接続端子２３ａには、ネットワーク１１に接続するＵＳＢケーブル２８が接続されている。

ここで、通信インタフェース２３は、パーソナルサーバ装置１とＰＣ２とがネットワーク１１を介して通信する機能、および、パーソナルサーバ装置１がＰＣ２を介して外部ネットワーク１２と通信する機能を提供する。また、指紋認証装置２２と指紋認証プログラム４２は個人認証手段を提供する。すなわち、指紋認証装置２２は指紋センサ部分２７で検出した使用者の指紋情報を読み取り、指紋認証プログラム４２は、読み取った指紋情報を予め登録された指紋情報と照合する。指紋情報が一致した場合には使用者が予め登録された使用者、本人であることが認証される。

サーバプログラム４３は、ＰＣ２との間でデータの処理を行うローカルサーバ機能と、外部ネットワーク１２との間でデータの処理を行うネットワークサーバ機能とを提供する。暗号プログラム４４は、指紋情報に基づいてパーソナルサーバ装置１に格納されるデータを暗号化するデータ暗号化手段を提供する。

図４はパーソナルサーバ装置のソフトウェア構成を表す概念図である。ハードウェアに、下層からＯＳ、データベース、データプロバイダインタフェース、フレームワーク、サービスプロバイダインタフェース、サービス、メッセージングＡＰＩが構成されている。

（携帯型パーソナルサーバ装置と通信端末との接続）

携帯型パーソナルサーバ装置１は、通信インタフェース２３によってＰＣ２と接続されることにより、ＰＣ側から電源が供給されて起動する。使用者は、指紋認証装置２２の指紋センサ部分２７に指先をあてて、指紋情報による個人認証を受ける。指紋認証装置２２が取得した読込指紋情報が予めパーソナルサーバ装置１に登録さ

れている登録指紋情報と一致した場合には、携帯型パーソナルサーバ装置１はネットワーク１１を介してＰＣ２と通信可能になる。

携帯型パーソナルサーバ装置１とＰＣ２は、ネットワーク１１を介して通信可能にするために、APIPA を用いてアドレスを取得する。この際、ＰＣ２に接続された外部ネットワーク１２とアドレスの衝突が起こらないよう協調してアドレッシングが行なわれる。ＰＣ２は、アドレッシングの後、Ｗｉｎｄｏｗｓ（登録商標）等のＰＣに実装されているリレーサービス２０を用いてディスカバリを行い、パーソナルサーバ装置１を発見する。ディスカバリを含め、携帯型パーソナルサーバ装置１とＰＣ２との間のコミュニケーションにはＳＯＡＰ（Simple Object Access Protocol）というプロトコルが利用される。その表現言語としては、ＸＭＬが用いられる。

ＰＣ２から携帯型パーソナルサーバ装置１が発見されると、外部ネットワーク１２と携帯型パーソナルサーバ装置１は通信することが可能になる。携帯型パーソナルサーバ装置１は、さらに、ネットワーク認証手段により、外部ネットワーク１２に対して固有の電子証明書を用いた接続作業を行う。この作業の結果、外部ネットワーク１２と携帯型パーソナルサーバ装置１との接続が確立されると、携帯型パーソナルサーバ装置１は外部ネットワーク１２上のネットワークサーバとして機能する。ネットワーク認証手段によって、外部ネットワーク１２からネットワークサーバとして機能している携帯型パーソナルサーバ装置１へアクセスしようとする他人や外部サーバ３は、携帯型パーソナルサーバ装置１が間違いなく当該携帯型パーソナルサーバ装置１の予め登録された使用者のものであることを確認できる。

ここで、ＰＣ２のリレーサービス２０は、ＰＣ２上のアプリケーションから携帯型パーソナルサーバ装置１、携帯型パーソナルサーバ装置１からＰＣ２上のアプリケーション、または携帯型パーソナルサーバ装置１から外部サーバ３等へのＳＯＡＰメッセージをリレーする。また、携帯型パーソナルサーバ装置１は、指紋認証装置２２で得た指紋情報をもとに公開鍵暗号方式に用いられる鍵の生成およびその保管を行う。また、必要に応じて共通鍵の生成をおこない、共通鍵、公開鍵の両方を

用いた通信暗号化の機能を提供する。

（作用効果）

使用者が携帯型パーソナルサーバ装置１を携帯することにより、常にデータとアプリケーションを当該携帯型パーソナルサーバ装置１に格納することができる。したがって、データを一元的に管理でき、特定のアプリケーションについて、ＰＣ自体にインストールすることなく、複数のＰＣから使用することが可能となる。

また、携帯型パーソナルサーバ装置１は、指紋情報による個人認証手段を有しているので、登録された持ち主以外はＰＣ２と接続してローカルサーバあるいはネットワークサーバとして動作させることができない。加えて、携帯型パーソナルサーバ装置１は固有の入出力装置も持たないので、持ち主本人以外は、格納されているデータにアクセスすることが難しく、情報の漏洩の危険がない。また、外部ネットワーク１２からネットワークサーバとして機能している携帯型パーソナルサーバ装置１へアクセスしようとする他人は、当該携帯型パーソナルサーバ装置１が間違いなく当該携帯型パーソナルサーバ装置１の予め登録された使用者のものであることを特定することができるので、通信システム１０の信頼性が高い。

さらに、携帯型パーソナルサーバ装置１は、通信システム１０において、ＴＣＰ／ＩＰでＰＣ２および外部ネットワーク１２と接続されてローカルサーバおよびネットワークサーバとして機能する。したがって、一般的なインターネット用ブラウザを用いて、相互動作が可能な形でユーザインタフェースを提供することができる。また、外部ネットワーク１２に接続されている外部サーバ３にデータやメッセージを受け渡して、外部サーバ３にあるプログラムを直接利用することができる。

さらにまた、携帯型パーソナルサーバ装置１と外部ネットワーク１２との接続には、ＰＣ２に実装されているリレーサービス２０を利用するだけなので、ＰＣ２にデータが一時的にも保管されることがない。したがって、ＰＣ２から情報が漏洩する危険性がない。

次に、携帯型パーソナルサーバ装置１は、一般の認証用デバイスやストレージデ

バイスと異なり、通常のサーバハードウェアと同様に、ＣＰＵ２１、フラッシュＲＯＭ２６、ＲＡＭ２４などから成るハードウェア構成を取っているため、内部のソフトウェア構成として標準的なアプリケーションサーバと同様の構成を採用することができる。また、固有のＣＰＵ２１を有しているため、ＰＣ２に負荷をかけることなく、携帯型パーソナルサーバ装置１内部のサービスを提供し、外部からの計算要求を処理し、自動的に計算処理結果を出力するといった通信システムを構築できる。

また、携帯型パーソナルサーバ装置１内部のサービスを提供するに当り、特殊なＡＰＩを使うのではなく、例えばＷ３Ｃにおいて定義されている標準的な Web Services の仕様に基づいたＡＰＩとして提供することが出来るので、サービス開発者は新たなプログラミング言語を学ぶ必要性がなく、携帯型パーソナルサーバ装置１の提供するサービスを使ったアプリケーションの開発、あるいはサービス自体の機能拡張作業等が容易である。

さらに、携帯型パーソナルサーバ装置１はＸＭＬ／ＳＯＡＰに対応し、固有のデータベースを保有するため、一般的なデータ通信システムとして用いることができる。また、開発したアプリケーションの汎用性が高い。また、携帯型パーソナルサーバ装置１は、ストレージメディアカードスロット２５を備えているので、必要に応じてメディアカードを入れ替えることにより、理論上無限大のストレージスペースを提供することが出来る。この場合でも、暗号プログラム４４は、指紋情報に基づいてメディアカードに格納されるデータを暗号化するので、データの機密性が高い。

さらにまた、携帯型パーソナルサーバ装置１とＰＣ２とを接続する通信インタフェース２３としてＵＳＢを用いているので、携帯型パーソナルサーバ装置１にＰＣ２から電源を供給することができる。したがって、自己電源を持つ必要がなく装置の小型化が図れる。また、充電等の必要もないので携帯に便利である。

（その他の実施の形態）

なお、上記の携帯型パーソナルサーバ装置１では、ＰＣ２との接続にＵＳＢを使用している。ＰＣとの間の物理的接続形態は無線、有線を問わず、例えば、イーサネット、Ｂｌｕｅｔｏｏｔｈ、ＷＬＡＮ、赤外線などが利用可能である。いずれの場合にも、ＳＳＬ通信などを用いてデータを全て暗号化することにより、通信のセキュリティを確保できる。

産業上の利用の可能性

本発明によれば、ユーザが携帯型パーソナルサーバ装置を携帯できるので、常にデータとアプリケーションを一元的に管理することができる。また、ＰＣなどのネットワーク接続手段を備えた通信端末と通信することによりローカルサーバ、ネットワークサーバとして機能するので、あらゆる場所に設置されているＰＣを用いて、携帯型パーソナルサーバ装置に格納されたデータとアプリケーションにアクセスすることができる。さらに、指紋センサなどの生体情報による個人認証手段を備えているので、持ち主以外は携帯型パーソナルサーバ装置をサーバ装置として機能させることができない。したがって、携帯型パーソナルサーバ装置を紛失した場合でも、格納されているデータに他人がアクセスすることはできないので、データの漏洩を避けることができる。また、ネットワークから携帯型パーソナルサーバ装置にアクセスしようとする他人は、そのネットワークサーバとして機能する携帯型パーソナルサーバ装置が常に持ち主本人のものであることを認識することができるので、通信の信頼性を確保することができる。

したがって、本発明の携帯型パーソナルサーバ装置を用いれば、分散型のネットワークサーバを用いたネットワークアプリケーションを利用する場合などにおいて、信頼性の高い通信システムを構築できる。

請求の範囲

１．　ネットワーク接続手段を備えた通信端末との間でデータ処理を行うローカルサーバ手段と、

前記通信端末のネットワーク接続機能によって当該通信端末に接続されたネットワークとの間で、データ処理を行うネットワークサーバ手段と、

生体情報に基づき個人認証を行う個人認証手段と、

前記個人認証手段により認証された場合にのみ、前記ローカルサーバ手段および前記ネットワーク手段を利用可能にする制御手段とを有している携帯型パーソナルサーバ装置。

２．　請求項１において、

前記個人認証手段は指紋センサなどの生体情報認識装置を備え、当該生体情報認識装置により読み込まれた読込生体情報が予め登録されている登録生体情報に一致するか否かにより個人認証を行う携帯型パーソナルサーバ装置。

３．　請求項２において、

格納データを前記読込生体情報を用いてデータを暗号化するデータ暗号化手段を有している携帯型パーソナルサーバ装置。

４．　請求項２において、

前記読込生体情報が前記登録生体情報に一致した場合に、前記読込生体情報に基づいて公開鍵暗号方式に用いられる鍵の生成と保管を行い、当該鍵を用いて送信されるデータを暗号化する通信暗号化手段を有している携帯型パーソナルサーバ装置。

５．　請求項１ないし４のうちのいずれかの項において、

前記通信端末に接続するための通信ケーブルを有しており、

前記通信ケーブルを介して前記通信端末から電源の供給を受ける携帯型パーソナルサーバ装置。

６．　請求項５において、

前記通信ケーブルはＵＳＢである携帯型パーソナルサーバ装置。

図 1

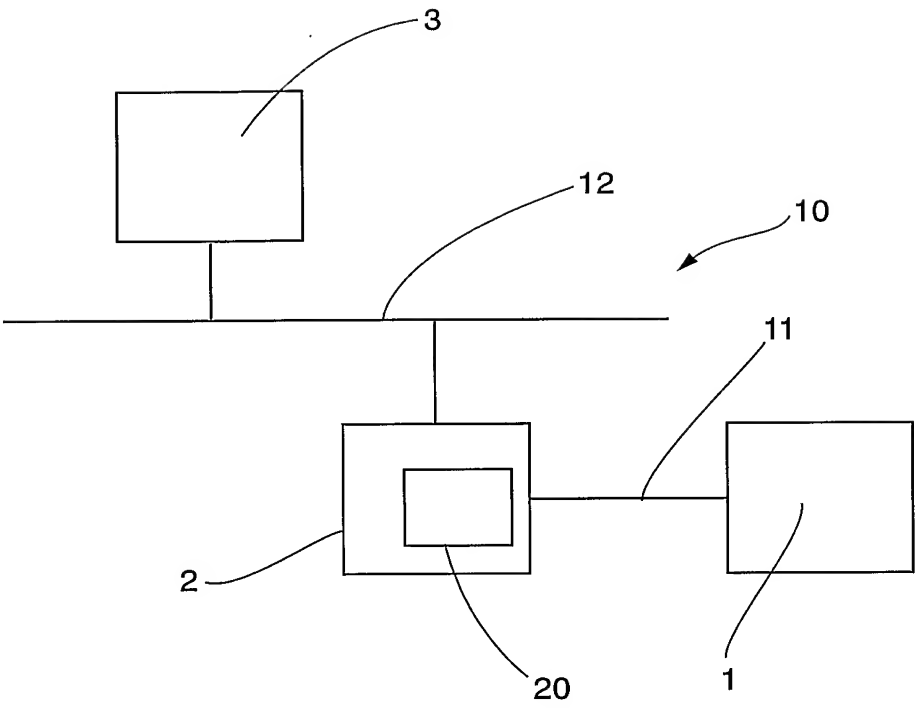


図２

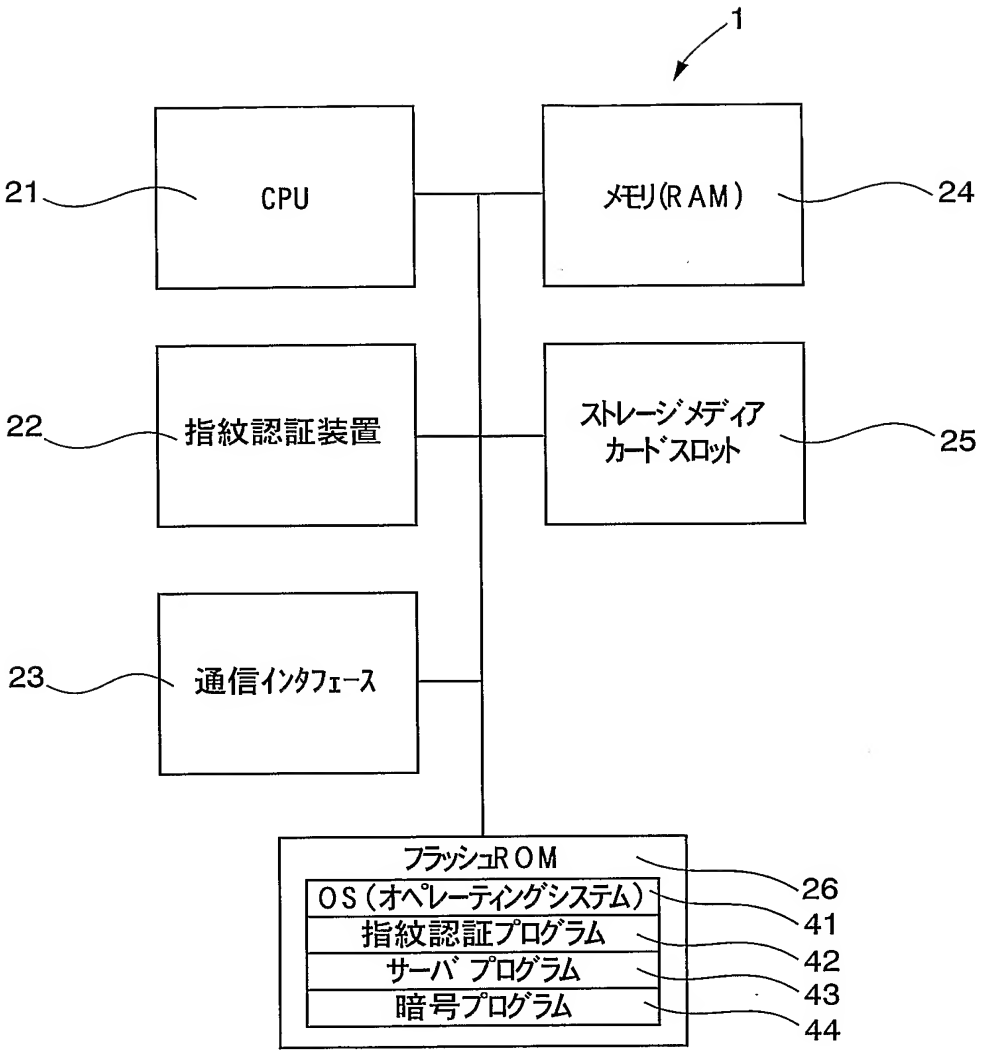

1
21
CPU
メモリ(RAM)
24
22
指紋認証装置
ストレージメディア
カードスロット
25
23
通信インタフェース
フラッシュROM
OS（オペレーティングシステム）
26
41
指紋認証プログラム
42
サーバ プログラム
43
暗号プログラム
44

図 3

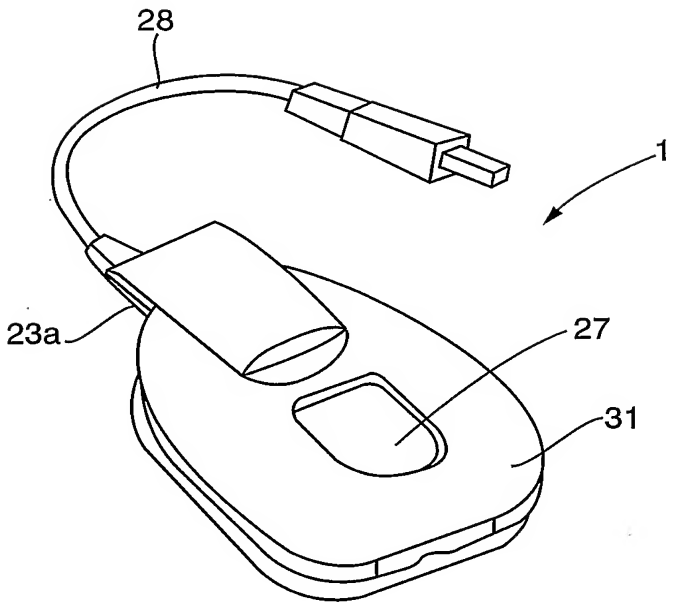
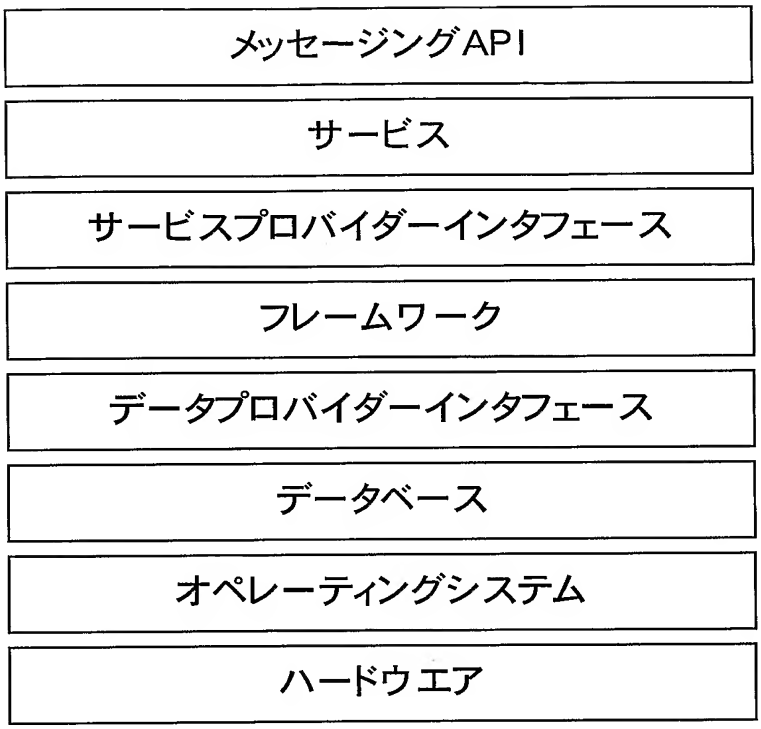


図4


メッセージングAPI
サービス
サービスプロバイダーインタフェース
フレームワーク
データプロバイダーインタフェース
データベース
オペレーティングシステム
ハードウエア

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/16815

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F15/00, G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F15/00, G06F1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Jitsuyo Shinan Toroku Koho 1996-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Toroku Jitsuyo Shinan Koho 1994-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-123437 A (Fujitsu Ltd.), 26 April, 2002 (26.04.02), Full text; all drawings (Family: none)	1-6
A	JP 2001-358828 A (Masahiko OKUNO), 26 December, 2001 (26.12.01), Full text; all drawings (Family: none)	1-6
A	JP 10-260749 A (Sun Micro Systems Inc.), 29 September, 1998 (29.09.98), Full text; all drawings & EP 853413 A2 & CN 1190215 A & SG 77151 A	1-6

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
06 April, 2004 (06.04.04)	20 April, 2004 (20.04.04)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/16815

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 11-316818 A (TRW Inc.), 16 November, 1999 (16.11.99), Full text; all drawings & EP 924657 A2 & US 6038666 A	1-6
A	JP 2001-92668 A (Sony Corp.), 06 April, 2001 (06.04.01), Full text; all drawings (Family: none)	1-6

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０３／１６８１５

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ　Ｃｌ⁷　Ｇ０６Ｆ１５／００，Ｇ０６Ｆ１／００

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ　Ｃｌ⁷　Ｇ０６Ｆ１５／００，Ｇ０６Ｆ１／００

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　　１９２６年－１９９６年
日本国公開実用新案公報　１９７１年－２００４年
日本国実用新案登録公報　１９９６年－２００４年
日本国登録実用新案公報　１９９４年－２００４年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	ＪＰ　２００２－１２３４３７　Ａ（富士通株式会社）２００２．０４．２６，全文，全図（ファミリーなし）	１－６
A	ＪＰ　２００１－３５８８２８　Ａ（奥野　昌彦）２００１．１２．２６，全文，全図（ファミリーなし）	１－６
A	ＪＰ　１０－２６０７４９　Ａ（サンマイクロシステムズ　インコーポレーテッド）１９９８．０９．２９，全文，全図 ＆ ＥＰ　８５３４１３　Ａ２　＆　ＣＮ　１１９０２１５　Ａ　＆ ＳＧ　７７１５１　Ａ	１－６

☒ Ｃ欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
０６．０４．２００４	20.4.2004

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	５Ｂ	９３６６
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	漆原　孝治 電話番号　０３－３５８１－１１０１　内線　３５４６		

国際調査報告	国際出願番号　ＰＣＴ／ＪＰ０３／１６８１５

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	ＪＰ　１１－３１６８１８　Ａ（ディーアールダブリュー・インコーポレーテッド）１９９９．１１．１６，全文，全図　＆ ＥＰ　９２４６５７　Ａ２　＆　ＵＳ　６０３８６６６　Ａ	１－６
Ａ	ＪＰ　２００１－９２６６８　Ａ（ソニー株式会社）２００１．０４．０６，全文，全図（ファミリーなし）	１－６